CENTER FOR BUSINESS & PUBLIC POLICY
GEORGETOWN UNIVERSITY McDonough SCHOOL of BUSINESS

Reply to Opposition in Response to the Petitions for Reconsideration

March, 2017

Larry Downes

Rafik B. Hariri Building • 37th and O Streets, NW • Washington, DC 20057
202.687.3686 • cbpp@georgetown.edu • cbpp.georgetown.edu • @GeorgetownCBPP

Before the FEDERAL COMMUNICATIONS COMMISSION

Washington, D.C. 20554

In the Matter of	**)**
	)
Protecting the Privacy of Customers of	**) WC Docket No. 16-106**
Broadband and Other Telecommunications	**)**
Services	**)**

Reply to Opposition in Response to the Petitions for Reconsideration

Larry Downes, Project Director
Georgetown Center for Business and Public Policy

March 16, 2017

Overview

The Commission should grant the Petitions for Reconsideration and withdraw the data collection and use rules adopted on October 27, 2016.[1] Petitioners raise numerous material economic, legal, and procedural defects in the Commission's 2016 Order.[2]

In response, opponents to the petitions simply rehash arguments raised and refuted in the original proceeding. No new facts or arguments have been made in support of the 2016 Order. Opponents ignore or mischaracterize the record, the nature of information collection and use in the digital ecosystem, and the substantial discord between the Commission's order and the long-standing data collection and use regime of the Federal Trade Commission.

As I have noted in several publications related to this proceeding,[3] opponents do not and cannot respond to three core errors in the Notice of Proposed Rulemaking[4] that infected the 2016 Order:

1. False Premise - The FCC proceeded under a fundamentally flawed premise, specifically that broadband providers, in contrast to content and other "edge" providers, are uniquely able to see and harvest users' "very sensitive and very personal" data and, on that basis, should be subject to more restrictive data collection and use rules than those applied by the Federal Trade Commission to other participants in the Internet ecosystem.

   In fact, thanks to a highly successful encryption campaign waged by many of the

---

[1] *In the Matter of Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*, WC Docket No. 16-106. REPORT AND ORDER, Adopted: October 27, 2016, Released: November 2, 2016. (*hereinafter* 2016 Order).

[2] *See* PETITION FOR RECONSIDERATION BY THE UNITED STATES TELECOM ASSOCIATION, WC Docket 16-106 (January 3, 2017); PETITION FOR RECONSIDERATION OF NCTA - THE INTERNET & TELEVISION ASSOCIATION, WC Docket 16-106 (January 3, 2017).

[3] *See* Reply Comments of Larry Downes, Project Director Georgetown Center for Business and Public Policy, *In the Matter of Protecting the Privacy of Customers of Broadband and Other Telecommunications Services,* WC Docket No. 16-106 (July 5, 2016); Larry Downes, *The Downside of the FCC's New Privacy Rules*, Harvard Business Review, May 27, 2016, available at https://hbr.org/2016/05/the-downside-of-the-fccs-new-internet-privacy-rules; Larry Downes, *FCC's Shifting Privacy Proposal A Trojan Horse For Discord,* Forbes, Oct. 25, 2016, *available at* https://www.forbes.com/sites/larrydownes/2016/10/25/fccs-shifting-privacy-proposal-a-trojan-horse-for-discord/#283494ed6ad9; Larry Downes, *Industry Groups Beg Congress, FCC To Restore Scrambled Privacy Rules,* Forbes, Jan. 30, 2017, *available at* https://www.forbes.com/sites/larrydownes/2017/01/30/industry-groups-beg-congress-fcc-to-restore-scrambled-internet-privacy-framework/print/ (attached as Appendix I).

[4] *In the Matter of Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*, WC Docket No. 16-106, NOTICE OF PROPOSED RULEMAKING, Adopted: March 31, 2016; Released: April 1, 2016 (hereinafter 2016 NPRM).

organizations who now oppose petitions for reconsideration, broadband providers are effectively blind to data traveling between users and the Internet.[5] Since the adoption of the 2016 Order, the encryption campaign has accelerated, further undermining the basis for the Order's extreme treatment of "sensitive" information to which ISPs increasingly do not have access.

2. Disharmony with the FTC – The Commission, in a "fact sheet" issued during the proceeding,[6] promised that its forthcoming rules would be "in harmony with other key privacy frameworks and principles – including those outlined by the Federal Trade Commission and the Administration's Consumer Privacy Bill of Rights." Yet even most opponents to the petitions for reconsideration acknowledge that the final order establishes a second and largely discordant regime for information collection and use.

   Though Internet content and service companies, outside the FCC's jurisdiction to regulate, are the true "gatekeepers" of users' information, the happy reality is that the kinds of abuses conjured by the 2016 Order to justify separate and more extensive limitations on data collection and use for ISPs have proven almost entirely hypothetical.

   This is due in large part due to the extensive and assertive oversight of data practices that has long been the province of the Federal Trade Commission and its adjudicative approach to privacy enforcement.

   The FCC replaced that functioning mechanism with prophylactic and highly constraining rules of its own—rules that only apply to broadband providers. This arbitrary approach, approved despite a nearly-total absence of economic analysis, does a great disservice to Internet users by subjecting the same information to two entirely different sets of rules and two entirely different approaches to enforcement.

3. The transaction costs of "opt-in" - The 2016 Order pre-emptively prohibits access providers from subsidizing user services through most forms of advertising-related business—the approach that has successfully driven the Internet and its "cycle of innovation" from the very beginning.

   Yet absent any economic analysis, the 2016 Order arbitrarily concluded that there were no relevant cost differences between the Commission's new opt-in regime and the FTC's

---

[5] *See* Peter Swire, Justin Hemmings, Alana Kirkland, *Online Privacy and ISPs: ISP Access to Consumer Data is Limited and Often Less than Access by Others*, The Institute for Information Security & Privacy at Georgia Tech (May 2016) (submitted in Docket No. WC 16-106).

[6] *Fact Sheet: Chairman Wheeler's Proposal to Give Broadband Consumers Increased Choice over their Personal Information,* October 6, 2016, *available at* https://apps.fcc.gov/edocs_public/attachmatch/DOC-341633A1.pdf

> long-standing opt-out regime.[7] Access providers, who have the least availability of data sources of any participant in the Internet ecosystem, are now required to obtain explicit consent from consumers before making nearly any use of information.
>
> As economists have long understood, the transaction costs associated with explicit opt-in regimes are, for most users and most uses, grossly inefficient. Many information exchanges that most users find valuable will be foregone, as the transaction costs of negotiating opt-in exceed the individual value of the exchange.[8]

Encryption and Asymmetry in Internet Advertising Markets

In opposition to the petitions for reconsiderations, opponents fail to respond to these defects, instead simply repeating specious arguments and misrepresenting the record as they did at the time of the original proceeding.

One particular example bears highlighting.

As the Commission learned in the course of the proceeding, broadband providers do not control, as the NPRM claimed, "the most important and extensive conduits of consumer information," giving them the ability to "threaten a person's financial security, reveal embarrassing or even harmful details of medical history, or disclose to prying eyes the intimate details of interests, physical presence, or fears."[9]

That's because, as unrefuted evidence in the record demonstrated, encryption of web and app traffic had already become nearly ubiquitous, with the sites consumers use most to store, share, and view sensitive information already fully compliant with the encrypted HTTPS protocol and end-to-end encryption on mobile devices.

The Commission had begrudgingly acknowledged in the NPRM that wide-scale encryption undermined the fundamental justification for any regulation of ISP data collection and use, let alone the extreme version ultimately adopted. As the NPRM noted:

> Indeed, the whole purpose of the customer-provider relationship is that the network becomes an essential means of communications with destinations chosen by the customer; which means that, ***absent use of encryption***, the

---

[7] *See* 2016 Order at ¶ 194 ("Although we recognize that opt-in imposes additional costs, based on these factors we find that opt-in is warranted to maximize opportunities for informed choice about sensitive information.")

[8] *See* Larry Downes, *A Rational Solution to the Privacy 'Crisis,'* POLICY ANALYSIS #716, January 7, 2013, *available at* http://object.cato.org/sites/cato.org/files/pubs/pdf/pa716.pdf.

[9] *2016 NPRM* at ¶ 2.

> broadband network has the technical capacity to monitor traffic transmitted between the consumer and each destination, including its content.[10]

Yet despite evidence of extensive and increasingly ubiquitous encryption provided by commenters on the NPRM, the FCC in the 2016 Order arbitrarily waived away its own admission:

> Also, contrary to some commenters' arguments, the existence of encryption on websites or even in apps does not remove browsing history from the scope of sensitive information…..While the record indicates that BIAS providers have a less granular view of encrypted web traffic than unencrypted, it does not change the breadth of the carrier's view….[11]

To buttress its pre-determined and arbitrary decision to treat web browsing and app history as sensitive information, the 2016 Order relied on the absurdly strained efforts of some commenters to describe how packet headers and IP addresses—all the providers can see, and then only when the user is not using a mobile device or a third-party Wi-Fi network—can theoretically be transformed into "a detailed composite portrait of a user's life,"[12] defeating the sole purpose of the encryption campaign in the first place.

The reality, as the record makes clear, is that ISPs have access to almost no data regarding a user's interactions with massively popular sites such as Facebook, Google, Instagram, Amazon, Apple, Twitter and YouTube. Only those companies have access to user data, of which, of course, they make extensive use to subsidize their services through customized advertising and to offer new and improved products based on analysis of user behavior.

Strangely, many of the organizations opposing petitions for reconsideration continue to argue both that encryption isn't happening and, if it is, that it is ineffective to shield consumers from similar data collection and use by ISPs.[13]

This is especially odd because these same organizations are the leaders in a highly-successful campaign to fully encrypt the web and mobile apps. They have, even since the Order was approved and the petitions for reconsideration filed, proudly boasted of the overwhelming

---

[10] *Id.* at ¶ 4 (emphasis added).

[11] *2016 Order* at ¶ 186.

[12] *See* Comments of Public Knowledge, the Benton Foundation, Consumer Action, Consumer Federation of America, and National Consumers League, May 27th, 2016, WC Docket 16-106 at pages 3-6.

[13] *See*, e.g., OPPOSITION OF THE CENTER FOR DEMOCRACY & TECHNOLOGY TO PETITIONS FOR RECONSIDERATION, WC Docket 16-106 (March 6, 2017) at p. 11 (hereinafter "CDT Opposition"); OPPOSITION TO PETITIONS FOR RECONSIDERATION filed by Access Humboldt, Access Now et. al (March 6, 2017) at pp. 2-3 (hereinafter "Coalition Opposition"); PUBLIC KNOWLEDGE, CENTER FOR DIGITAL DEMOCRACY, AND BENTON FOUNDATION'S OPPOSITION TO PETITIONS FOR RECONSIDERATION, WC Docket 16-106 (March 6, 2016) at p 3.

accomplishments of their efforts—success they now ignore or dismiss in their opposition to the petitions for reconsideration.

The Center for Democracy and Technology, for example, argues in its opposition that "Petitioners erroneously argue that encryption technologies effectively block ISPs from having a comprehensive view of customers' online activities."[14]

Yet in an extensive "Issue Brief" published by CDT just prior to passage of the 2016 Order says just the opposite, noting that HTTPS encryption stops ISPs from doing precisely the kinds of data analysis that the websites who have adopted the standard can continue doing:

> **Without HTTPS, ISPs and governments can spy on what your users are doing:** Traffic on the web traverses many different networks from server to browser, and each of these networks (or equipment installed on these networks) can see the full contents of unencrypted (HTTP) traffic. This means ISPs can do things like monitor your web traffic to build advertising profiles.[15]

And while CDT's Opposition vaguely states in support of the 2016 Order that "a significant amount of internet traffic remains unencrypted," CDT's own Chief Technologist said in a 2015 interview that "over half of all web traffic is now secured and that by the end of the year, that number would climb to 70%." He also noted that most email is already encrypted, as is Skype and consumer interactions with Netflix and, "increasingly, the videos you watch." In the next five to 10 years, he said, "encryption will become ubiquitous."[16]

Those optimistic predictions were recently underscored by the Electronic Frontier Foundation, one of the signatories to the Coalition Opposition. Though the Coalition now says encryption data supplied to the Commission during the proceeding has been "refuted,"[17] a post on EFF's own website dated just one week before reached a very different conclusion, providing its own data to support the view that ISPs have become largely blind—one of the explicit goals of the encryption campaign:

> The movement to encrypt the web has reached a milestone. As of earlier this month, approximately half of Internet traffic is now protected by HTTPS. In other

---

[14] *CDT Opposition* at p. 11.

[15] Center for Democracy and Technology, *Issue Brief: The Time Has Come to Move to HTTPS!*, October 6, 2016, *available at* https://cdt.org/insight/issue-brief-the-time-has-come-to-move-to-https/. *See* also *Working Together to Make The Entire Internet More Secure,* Center for Democracy and Technology, January 25, 2017, *available at* https://cdt.org/blog/working-together-to-make-the-entire-internet-more-secure/. ("Based on the response, it looks like a number of the major adult sites are going to take CDT, Mozilla, and Wired up on our offer to help make the move to HTTPS. Awesome.")

[16] *See* Larry Downes, *FCC Shifting Privacy Proposal a Trojan Horse for Discord*, Forbes, October 25, 2016, *available at* https://www.forbes.com/sites/larrydownes/2016/10/25/fccs-shifting-privacy-proposal-a-trojan-horse-for-discord/#283494ed6ad9.

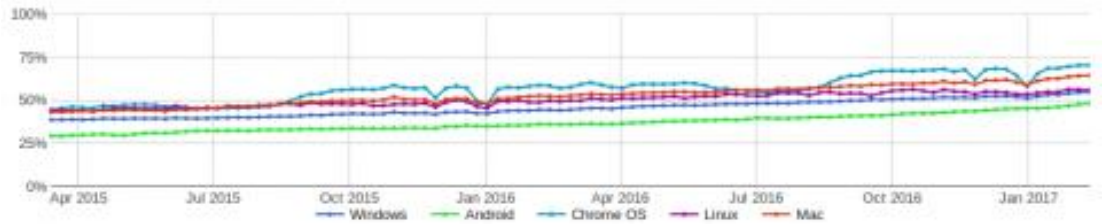
[17] Coalition Opposition at p. 3.

words, we are halfway to a web safer from the eavesdropping, content hijacking, cookie stealing, and censorship that HTTPS can protect against.

Mozilla recently reported that the average volume of encrypted web traffic on Firefox now surpasses the average unencrypted volume.

Source: https://letsencrypt.org/stats/

Google Chrome's figures on HTTPS usage are consistent with that finding, showing that over 50% of of [sic] all pages loaded are protected by HTTPS across different operating systems.



Source: https://www.google.com/transparencyreport/https/metrics/

This milestone is a combination of HTTPS implementation victories: from tech giants and large content providers, from small websites, and from users themselves.[18]

Opponents claim both that ISPs have almost supernatural abilities to collect an "intimate, all-encompassing picture window into its customers' behavior,"[19] and, at the same time, that they

[18] Electronic Frontier Foundation, *We're Halfway to Encrypting the Entire Web*, Feb. 21, 2017, *available at* https://www.eff.org/deeplinks/2017/02/were-halfway-encrypting-entire-web.

[19] *See* Opposition to Petitions for Reconsideration of ConsumersUnion and Consumer Federation of America, WC Docket 16-106 (March 6, 2017) at p. 2. ConsumersUnion and Consumer Federation of America continue: "As data storage costs continue to shrink, there is less natural disincentive to stop BIAS providers from simply saving all data

have succeeding in coordinating every constituency in the Internet ecosystem to encrypt their traffic, making it invisible to ISPs and anyone else, other than the sites and services providing the encrypted interactions.

Opponents cannot have it both ways. The reality, as they know, is that unlike most websites, smartphone apps, Internet-based services and leading advertising platforms, ISPs are largely blind to the Internet activities of their customers--precisely as their campaign promised.

Thanks to the widespread adoption of HTTPS and end-to-end encryption, as opponents elsewhere boast, ISPs alone are unable to "monitor your web traffic to build advertising profiles." The "victories" in the HTTPS campaign have come from coordination by opponents of everyone "from tech giants and large content providers, from small websites, and from users themselves."

Yet opponents continue to argue disingenuously that ISPs, with supposedly complete access to consumer Internet activity, must be held to a higher standard of information collection and use, and in particular to an economically-crippling "opt-in" regime. The data did not support that conclusion at the time the 2016 Order was adopted. And evidence reported since then—collected and, when convenient, cited with pride by opponents to the petitions for reconsideration—makes clear that argument has now fully evaporated.

The reality, implied if not explicit in all opponent filings, is that ISPs are distinct and require excessive regulation not because of their privileged position relative to consumers but for another, more pragmatic reason: ISPs are the only entity in the Internet ecosystem subject to the jurisdiction of the FCC. They are, therefore, the only group on whom the FCC can impose these costly regulations.

Indeed, many of those opposing the petitions for reconsideration have here and elsewhere expressed an explicit desire to extend the opt-in regime to all participants in the Internet ecosystem, if only doing so were legally and politically feasible.[20]

Fortunately, it isn't. Because the economics are clear, and weigh heavily in favor of harmony with longstanding regulatory approach. The economic foundation of the Internet and its

---

they transmit, amassing year upon year of wide-ranging intimate, personal, and sensitive information about millions and millions of captive broadband customers, and retaining it indefinitely." But there is no business value to saving encrypted data the BIAS provider cannot, by definition, access.

[20] *See*, e.g., Coalition Opposition at pp. 4-5 ("[T]he record reflected consumer skepticism of current privacy regimes. For instance, even under the FTC's privacy regime, consumers still modified their behavior online to prevent losing control of data, and expressed a desire for more privacy protections enforced by government entities. Thus, it is simply incorrect to claim, as so many petitioners do, that the FTC's regime is successful.") (footnotes omitted)

remarkable productivity has been based almost entirely on the ability of companies to make wide use of contextual information, including consumer behavior, and to collect and use that information on an opt-out basis to provide maximum flexibility with minimum transaction costs.[21]

The principal result of the very different data collection and use regime applied to ISPs by the 2016 Order, compared to all other participants in the Internet ecosystem, will not be improved information protection and choice for consumers. Rather, its chief effect will be to saddle ISPs hoping to enter and compete in the digital advertising market with a significant competitive disadvantage.

There is no dispute that the digital advertising market is highly concentrated, dominated today by just two companies.[22] Consumers would, therefore, directly benefit from uniform, technology-neutral policies that encourage competition, making it possible for ISPs, like every other digital entity, to offer subsidized, self-improving products and services based on information collection and use, including advertising.

One would think that consumer advocacy groups committed to expanding competition in the digital ecosystem would support policies that make it easier, not harder, for new entrants to break into highly concentrated markets.

But that is not a mystery the Commission need resolve. If nothing else, the continued success of opponents' encryption campaign, as reported by the opponents themselves, constitutes new information unavailable to the Commission at the time of the 2016 Order. Its goal is to keep from ISPs the kind of contextual data that other Internet companies have used successfully for two decades to create new products and subsidize their free content and services through advertising.

And it is, as opponents themselves have reported with pride, succeeding even better and faster than expected.

---

[21] Larry Downes, *A Rational Solution to the Privacy 'Crisis,'* POLICY ANALYSIS #716, January 7, 2013, *available at* http://object.cato.org/sites/cato.org/files/pubs/pdf/pa716.pdf.

[22] *See*, e.g., Sarah Fischer, *Duopoly watch: Google and Facebook gobble up even more ad dollars,* Axios, March 15, 2017, available at https://www.axios.com/google-facebook-gobbling-up-even-more-ad-dollars 2314107978.html; Peter Kafka, *Google and Facebook are Booming. Is the Rest of the Digital Ad Business Shrinking?,* Recode, Nov. 10, 2016, *available at* http://www.recode.net/2016/11/2/13497376/google-facebook-advertising-shrinking-iab-dcn.

That irrefutable reality constitutes an independent basis for granting the petitioners' requests for reconsideration.

Respectfully Submitted,

Larry Downes
Project Director
Evolution of Regulation and Innovation Project
Georgetown Center for Business and Public Policy

Attachment

Appendix I

Forbes


Larry Downes Contributor

Tech 1/30/2017 @ 6:00AM

Industry Groups Beg Congress, FCC To Restore Scrambled Internet Privacy Rules

Late last week, a diverse coalition of advertising trade groups, broadband providers and advocacy groups across the political spectrum moved to reverse the FCC's last-minute effort to radically alter the flow of consumer information, which would have reversed the "notice and choice" model for ad-based services that constitutes the core of the commercial Internet.

The FCC's privacy order, adopted a few days before the November election, was one of several late efforts by the Obama administration to rewrite long-standing pillars of Internet governance, many of which flowed from the Commission's controversial decision two years ago to "reclassify" broadband as a public utility subject to thousands of regulations written for the former Bell monopoly in the 1930's.

At the time, the Commission's then-Chairman Tom Wheeler promised the sweeping powers would only be used to enforce the agency's open Internet rules, sometimes referred to as "net neutrality."

But soon after, Wheeler's pledge to forbear from interfering in Internet governance, historically left to engineering groups and other regulators including the Federal Trade Commission, proved ephemeral.

The challenged FCC order enacted rules that required ISPs—and only ISPs—to secure permission from individual consumers before using contextual information for advertising and related purposes. The FCC's unique and complicated "opt-in" approach flipped the wildly successful "opt-out" framework established decades ago by the FTC, which has fueled free social media applications and other content at the heart of the Internet's wildly successful growth and innovation.

Earlier in the week, advertisers and carriers asked Congress to nullify the privacy order under the Congressional Review Act, a request seconded by a coalition of advocacy groups. On Friday, meanwhile, broadband access providers filed papers asking the FCC to stay enforcement of the new rules while the Commission reconsiders the order based on previously-filed objections.

At the same time, the groups—representing nearly every ISP in the country—issued a statement reaffirming their commitment to the FTC framework, which they noted "has protected internet users for years and provided the flexibility necessary to innovate new product solutions to enhance consumers' online experiences."

That pledge is by no means rhetorical. As one of many unfortunate side-effects of the FCC's public utility reclassification, the FTC was stripped of its long-standing authority over ISPs to enforce anti-competitive and anti-consumer laws and regulations.

As I wrote just before the Commission voted to approve the privacy measure, the shifting proposal suffered from other legal and procedural defects that are now the basis for multiple requests to reconsider the order.

On the substance, the final order represented a dangerous break from the FTC framework, as noted by the FTC's own staff and some of its Commissioners, including Maureen Ohlhausen, who was named last week as Acting Chairman of the agency.

As Ohlhausen said in a speech last year, before the FCC cut them out of the picture, her agency had already brought "more than 150 privacy and data security enforcement actions, including actions against ISPs and against some of the biggest companies in the internet ecosystem," comprising giants in search, advertising, content and e-commerce.

The FCC's privacy regulations bizarrely restricted only ISPs, who so far have done little in the way of contextual advertising, severely limiting their ability to create new free or subsidized services just as established Internet information and service providers have done for years, including search engines, social media, e-commerce, email, messaging and other free or subsidized content providers.

The exchange of contextual information for free or subsidized access has largely fueled the commercial Internet from its beginnings, forming an important or often the sole basis of revenue for companies as different as Facebook, Google, Instagram, Amazon, Apple, Twitter and YouTube.

Besides restricting the continued use of a business models that consumers have clearly embraced, the FCC's actions subjected different parts of the Internet ecosystem to wildly different rules for information collection and use for no particular reason and in ways almost certain to leave consumers confused as to both the what and who of permitted information collection, use, and enforcement.

In issuing its incompatible order over the concerns of nearly every constituent part of the Internet ecosystem, including Google, the FCC ignored overwhelming evidence that broadband providers were already strongly handicapped in efforts to leverage information and so-called "big data" to create new services.

That's because a successful campaign to encrypt interactions between Internet users and service providers, accelerated in response to the revelations of Edward Snowden, has left ISPs nearly blind to the specifics of user interactions with leading websites and services.

According to the Joseph Lorenzo Hall, Chief Technologist at the Center for Democracy and Technology, over half of all web traffic is now secured, as invisible to ISPs as it is to the NSA. By the end of this year, that number will climb to 70%. Most email is already encrypted. Skype is encrypted, as are your interactions with Netflix and, increasingly, the videos you watch. In the next five to 10 years, Hall says, encryption will become ubiquitous.

The FCC's midnight push to undo the FTC's well-regarded information collection and use framework is not the only action by former Chairman Wheeler that now finds itself in the legal crosshairs.

The FCC late last year also unwound nearly twenty years of light-touch regulation for highly competitive business data services, subjecting even new entrants who have invested heavily in high-speed technologies to potential rate regulation and micromanagement of contract terms and conditions.

In the final days before Wheeler's resignation, a bureau report signaled concerns with mobile services, sometimes known as "zero-rating," that allow consumers to enjoy a wide range of audio and video content that doesn't count towards their data plans.

All of these initiatives were based on the agency's newly-discovered public utility authority. The FCC's new Chairman Ajit Pai, who has served as a Commissioner for the past five years and who objected to each of these divergences, is likely to revisit all of them, including Wheeler's controversial claim that these sweeping powers had been granted by Congress all along and had simply gone unnoticed by previous Chairmen.

Even before the election, many of the Commission's most controversial and legally-dubious initiatives had fallen to court challenges the agency wisely chose not to appeal. These included rules that pre-empted states from regulating expensive and largely failed municipal broadband projects, arbitrary new rates for prison telephone services, and a plan to force pay TV providers to provide programming content and user viewing habits to third party services in violation of U.S. copyright law.

The public utility order—the lynchpin for many of the most ill-considered initiatives in Wheeler's campaign—is itself under fire. A D.C. appellate court is still considering a request to rehear the case after a three-judge panel upheld it last year. Meanwhile, Congress and the FCC itself are almost certain to consider alternatives to ensuring enforceable net neutrality rules that don't rely on public utility authority.

In retrospect, the public utility order may prove the unraveling of Wheeler's legacy. In 2014, the same D.C. court had told the agency, in rejecting a 2010 attempt to enact net neutrality rules, that it had adequate authority to secure them under a much more limited provision of the law.

Wheeler characterized that decision as a "roadmap" he intended to follow to quickly and permanently secure enforceable rules and end a decade-old debate about the agency's jurisdiction over network management practices.

But under unprecedented pressure from the White House later that year, Wheeler reversed course and discarded the court's guidelines, as well as an offer from leading Republicans to pass legislation that would make net neutrality a matter of federal law.

Now, with a new FCC and a White House committed to reducing regulatory drag on the economy, that decision increasingly appears to have been a very bad gamble, one that provided no benefit to Internet users.

Time will tell. Perhaps, as with the FCC's flirtation with a radically different privacy framework, very little time.